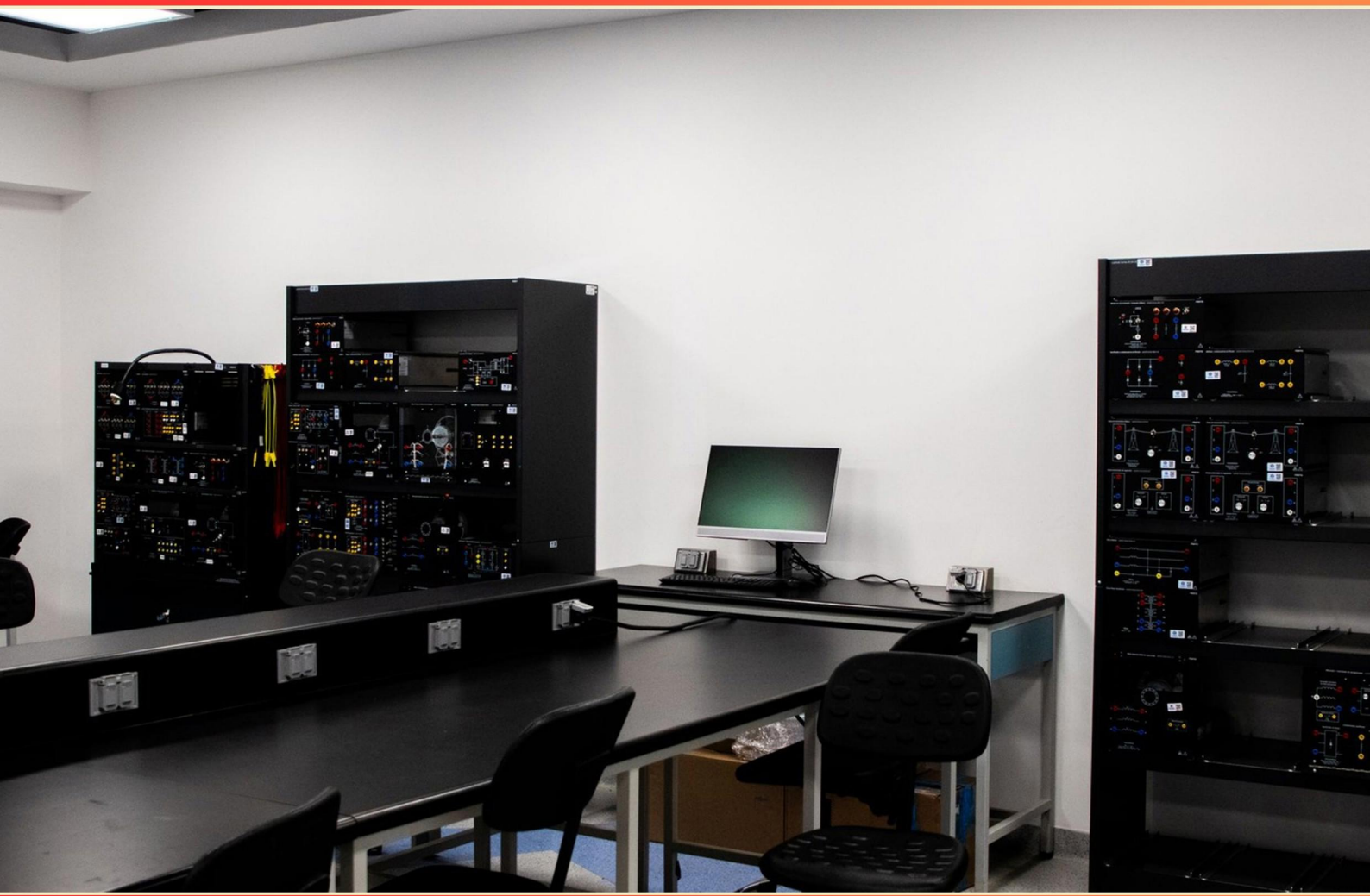
SANS GLOBAL INDUSTRIAL CYBER SECURITY PROFESSIONAL (GICSP) PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://sansgicsp.examzify.com

Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

SAMPLE

Table of Contents

Copyright 1

Table of Contents 2

Introduction 3

How to Use This Guide 4

Questions 5

Answers 8

Explanations 10

Next Steps 16

SAMPLE

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- Practice answering questions under realistic conditions,
- Improve accuracy and speed,
- Review explanations to strengthen weak areas, and
- Approach the exam with greater confidence.

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

SAMPLE

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here's how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don't just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There's no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

SAMPLE

Questions

SAMPLE

1. What is a unique feature of Wireless HART security?

A. It uses the same key for all devices

B. It restricts joins by key, manufacturer, and product name/tag

C. It transmits data unencrypted

D. It requires physical access for configuration

2. What should a well-defined training program for security awareness primarily include?

A. Employee recreational activities

B. Formal procedures and facility training

C. Training only on technical skills

D. Optional participation for employees

3. Which wireless standard was developed by ISA to compete with Wireless HART?

A. Bluetooth

B. Zigbee

C. ISA100.11a

D. WiFi

4. What is the acceptable throughput rate for biometrics?

A. 5 per minute

B. 10 per minute

C. 15 per minute

D. 20 per minute

5. Which of the following accurately describes the functionality of an Account?

A. It provides unlimited access to all system resources

B. It allows a user to authenticate for authorized service access

C. It is a fixed system feature for data storage

D. It offers monitoring for user activity

SAMPLE

6. Which Python-based framework is associated with Zigbee security?

A. KillerBee

B. AirSnort

C. WEPCrack

D. SniffingTool

7. Which of the following is considered a management protocol in an ICS environment?

A. HTTP

B. SMTP

C. SNMP

D. FTP

8. Which access control model allows permissions based on a lattice structure?

A. Biba Integrity Model

B. Take-Grant Model

C. Lattice Model

D. Clark-Wilson Model

9. What characteristic defines an effective cryptosystem?

A. The encryption process is time-consuming

B. It requires complex user training

C. The strength depends on the secrecy of keys

D. The algorithm itself must remain secret

10. Which ICMP type signifies a ping request?

A. Type 0

B. Type 8

C. Type 3

D. Type 5

SAMPLE

Answers

SAMPLE

1. B
2. B
3. C
4. B
5. B
6. A
7. C
8. C
9. C
10. B

SAMPLE

Explanations

SAMPLE

1. What is a unique feature of Wireless HART security?

A. It uses the same key for all devices

B. It restricts joins by key, manufacturer, and product name/tag

C. It transmits data unencrypted

D. It requires physical access for configuration

Wireless HART security incorporates several important features to ensure the integrity and confidentiality of data in industrial settings. A standout aspect of this system is its ability to restrict network access based on specific criteria such as key, manufacturer, and product name or tag. This method of restriction is crucial for enhancing the security of the network because it helps to prevent unauthorized devices from joining and communicating over the network. By implementing join restrictions, Wireless HART ensures that only authorized devices can interact with the network, thereby mitigating risks associated with rogue devices or potential breaches. This is particularly important in industrial environments where the consequences of unauthorized access could be significant. The feature of restricting joins by key, manufacturer, and product name/tag adds an additional layer of security to the network, allowing for a more controlled and secure operational environment. This protects sensitive data and maintains the operational integrity of the connected devices.

2. What should a well-defined training program for security awareness primarily include?

A. Employee recreational activities

B. Formal procedures and facility training

C. Training only on technical skills

D. Optional participation for employees

A well-defined training program for security awareness primarily includes formal procedures and facility training because it ensures that employees are adequately educated on the specific protocols and security measures relevant to their organization. This type of training typically covers the policies, procedures, and best practices employees must follow to mitigate risks and respond effectively to security threats. Formal procedures provide a structured approach to security that includes how to handle sensitive information, recognize potential threats, and understand the organization's overall security posture. Facility training may involve practical instructions on dealing with security technologies and emergency procedures, thus equipping employees with the skills they need to act confidently and appropriately in various scenarios. In contrast, recreational activities, training only on technical skills, and optional participation do not contribute to a comprehensive security awareness program. Recreational activities do not address the critical need for employees to understand and comply with security measures. Training exclusively focused on technical skills may leave gaps in understanding organizational policies, while optional participation could risk leaving some employees uninformed and unprepared to react to security incidents. Such gaps can lead to vulnerabilities that compromise the organization's security.

SAMPLE

3. Which wireless standard was developed by ISA to compete with Wireless HART?

A. Bluetooth

B. Zigbee

C. ISA100.11a

D. WiFi

The correct answer is ISA100.11a because this wireless standard was specifically developed by the Instrumentation, Systems, and Automation Society (ISA) to provide a robust solution for industrial wireless communications, directly competing with Wireless HART. ISA100.11a offers features that cater to the needs of industrial environments, such as the ability to handle a variety of applications, support for secure and reliable data transmission, and interoperability with various devices. Moreover, ISA100.11a employs a highly flexible networking technology capable of addressing the challenges posed by industrial operations, including scalability, energy efficiency, and robust performance in difficult radio environments. While options like Bluetooth, Zigbee, and WiFi are also wireless communication standards, they were not developed specifically to meet the requirements of industrial process automation in the same way as ISA100.11a. Bluetooth is primarily designed for short-range personal area networking, Zigbee focuses on low-power applications for sensor networks, and WiFi is geared more towards general internet connectivity rather than the specialized needs of industrial settings.

4. What is the acceptable throughput rate for biometrics?

A. 5 per minute

B. 10 per minute

C. 15 per minute

D. 20 per minute

The acceptable throughput rate for biometrics is identified as 10 per minute. This rate reflects a balance between security and practicality in biometric systems, ensuring that users can be authenticated efficiently without significant wait times. Biometrics are increasingly used in access control systems to authenticate individuals based on unique physical characteristics such as fingerprints, iris patterns, or facial recognition. A throughput rate of 10 per minute allows organizations to manage security effectively while keeping lines moving and minimizing disruptions in high-traffic scenarios. Throughput rates significantly lower than this could lead to delays, increased frustration among users, and potential bottlenecks, especially in environments where quick access is necessary, such as airports or secure facilities. Conversely, throughput rates that are too high may compromise the thoroughness of the authentication process, allowing for potential security breaches. Therefore, 10 per minute is seen as a balanced rate that maintains both security integrity and user convenience.

SAMPLE

5. Which of the following accurately describes the functionality of an Account?

A. It provides unlimited access to all system resources

B. It allows a user to authenticate for authorized service access

C. It is a fixed system feature for data storage

D. It offers monitoring for user activity

The functionality of an account is fundamentally tied to its role in user access management within a system. An account is primarily designed to allow users to authenticate their identity, enabling them to access specific services and resources for which they have been authorized. This process is integral to maintaining security and ensuring that users can only interact with parts of the system permissible to them, based on their roles and permissions. When a user successfully authenticates using their account credentials, they gain access to the applications, data, and resources that they are permitted to use. This mechanism is crucial in environments such as industrial control systems, where safeguarding sensitive data and operational integrity is paramount. Other options present aspects that are not accurate representations of an account's primary functionality. Unlimited access to all system resources misrepresents the nature of user permissions, which are intended to be restricted according to role requirements. The notion of a fixed feature for data storage does not pertain to authentication processes, while monitoring user activity, although important for security, is a separate function often handled by auditing or monitoring tools, rather than being a direct characteristic of an account itself. Therefore, the essence of an account lies in facilitating authenticated access to services, which is accurately captured in the correct answer.

6. Which Python-based framework is associated with Zigbee security?

A. KillerBee

B. AirSnort

C. WEPCrack

D. SniffingTool

KillerBee is a Python-based framework specifically designed for research and development around Zigbee and other low-power wireless networks. It provides tools for sniffing, injecting, and analyzing Zigbee packets, making it invaluable for security assessments of Zigbee communications. The framework facilitates the exploitation and analysis of vulnerabilities within Zigbee networks, which are commonly used in industrial control systems and IOT applications. Understanding Zigbee security is particularly important in the context of industrial cyber security, as these networks are often part of critical infrastructure that requires robust protection against attacks. KillerBee's capabilities allow security professionals to simulate attacks and test the resilience of Zigbee-enabled devices, aiding in the identification and mitigation of risks associated with wireless communications. Other options mentioned serve different purposes or focus on different technologies. For instance, AirSnort and WEPCrack deal primarily with security in wireless networks (WEP encryption), while SniffingTool, while potentially useful for general packet sniffing, does not specialize in Zigbee and lacks the tailored features KillerBee offers for this specific kind of network vulnerability assessment.

SAMPLE

7. Which of the following is considered a management protocol in an ICS environment?

A. HTTP

B. SMTP

C. SNMP

D. FTP

The correct choice is based on the specific role of the protocol in managing devices within an Industrial Control System (ICS) environment. Simple Network Management Protocol (SNMP) is specifically designed for managing and monitoring network devices, which makes it a vital tool in the context of ICS. It operates by allowing network devices to exchange management information and provides functionalities such as status monitoring and notifications for network events or failures. In an ICS setup, the ability to monitor and collect data about the status and performance of devices and processes is crucial for maintaining operational efficiency and safety. SNMP provides a standardized way to perform these tasks, allowing operators to configure and manage devices such as routers, switches, and servers effectively. The other protocols listed—HTTP, SMTP, and FTP—are primarily used for data transfer and communication rather than management. HTTP is used for web traffic, SMTP is focused on email transmission, and FTP is used for transferring files between systems. While these protocols may have their place in an ICS environment for other functionalities, they do not serve the specific purpose of device management as effectively as SNMP does. This is why SNMP is recognized as a management protocol in the context of ICS.

8. Which access control model allows permissions based on a lattice structure?

A. Biba Integrity Model

B. Take-Grant Model

C. Lattice Model

D. Clark-Wilson Model

The correct answer is C, and this relates to the way permissions and access rights are structured within a lattice-based approach. The Lattice Model is specifically designed to provide a framework for access control that incorporates different levels of permissions organized hierarchically. In this model, each subject (such as a user or process) and each object (such as files or databases) is assigned a sensitivity label, which denotes the level of access that is appropriate. The main concept behind the lattice structure is that it allows users to access objects at or below their level of security clearance while preventing access to objects above it. This ensures that information does not flow from a higher security level to a lower one, thereby maintaining confidentiality and integrity. By incorporating this structured hierarchy and clear definitions of access levels, the Lattice Model offers a robust means of enforcing security policies that require strict adherence to defined permissions based on this lattice concept. The other models referenced have different principles and may not utilize this structured approach to permissions, making the Lattice Model uniquely suited for scenarios where precise security classifications are essential.

SAMPLE

9. What characteristic defines an effective cryptosystem?

A. The encryption process is time-consuming

B. It requires complex user training

C. The strength depends on the secrecy of keys

D. The algorithm itself must remain secret

An effective cryptosystem is fundamentally defined by the strength of its security, which is primarily dependent on the secrecy of the keys used in the encryption and decryption processes. When the keys are kept secret and are sufficiently complex, they ensure that unauthorized parties cannot decrypt the information without access to these keys. This principle is rooted in the concept of "Kerckhoffs's principle," which states that a cryptographic system should remain secure even if everything about the system except the key is public knowledge. Thus, even if the algorithm is known, the security of the system will remain intact as long as the key remains secret. The other characteristics mentioned do not contribute to the effectiveness of a cryptosystem in the same way. The encryption process being time-consuming does not necessarily indicate a secure system; rather, efficiency can be crucial in practical applications. Similarly, complex user training can create barriers to proper implementation and usage rather than enhancing security. Lastly, while keeping an algorithm secret may seem beneficial, many secure systems rely on public algorithms whose security is based on the complexity and secrecy of the keys, rather than the obscurity of the algorithm itself.

10. Which ICMP type signifies a ping request?

A. Type 0

B. Type 8

C. Type 3

D. Type 5

The Internet Control Message Protocol (ICMP) is primarily used for sending error messages and operational information in network settings. A ping request is a specific use of ICMP that checks the reachability of a host on an IP network and measures the round-trip time for messages sent to that host. The correct type for a ping request is Type 8, also known as the Echo Request message. When a system sends an ICMP Echo Request (Type 8), it typically expects a response back from the target, which is indicated by an Echo Reply, denoted as Type 0. This functionality allows network administrators to diagnose connectivity issues and assess the status of devices within a network. In the context of ICMP message types: - Type 0 is used for Echo Replies, responding to requests. - Type 3 represents Destination Unreachable messages, which indicate that a destination cannot be reached. - Type 5 is used for Redirect messages, which inform a host to send packets to a more efficient route. Thus, Type 8 being the correct response signifies the specific function of initiating a ping request within the networking framework.

SAMPLE

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://sansgicsp.examzify.com

We wish you the very best on your exam journey. You've got this!

SAMPLE